Sonderbedingungen für das PSD OnlineBanking

PSD Bank München eG, Sitz Augsburg

Stand: Januar 2018

1. Leistungsangebot

(1) Der Konto-/Depotinhaber und dessen Bevollmächtige können Bankgeschäfte mittels OnlineBanking in dem von der Bank angebotenen Umfang abwickeln. Zudem können sie Informationen der Bank mittels OnlineBanking abrufen. Der Inhaber eines Zahlungskontos und dessen Bevollmächtigte sind zusätzlich berechtigt, für die Auslösung eines Zahlungsauftrages einen Zahlungsauslösedienst gemäß § 1 Absatz 33 Zahlungsdiensteaufsichtsgesetz zu nutzen und für die Mitteilung von Informationen über ein Zahlungskonto einen Kontoinformationsdienst gemäß § 1 Absatz 34 Zahlungsdiensteaufsichtsgesetz zu nutzen.

(2) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer" bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto" bezeichnet, es sei denn, dies ist im Folgenden ausdrücklich anders bestimmt.

(3) Zur Nutzung des OnlineBanking gelten die mit der Bank gesondert vereinbarten Verfügungslimite. Eine Änderung dieser Limite kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

2. Voraussetzungen zur Nutzung des OnlineBanking

Der Teilnehmer benötigt für die Nutzung des OnlineBanking die mit der Bank vereinbarten Personalisierten Sicherheitsmerkmale und Zahlungsinstrumente, um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen (siehe Nummer 3) und Aufträge zu autorisieren (siehe Nummer 4). Statt eines Personalisierten Sicherheitsmerkmals kann auch ein biometrisches Merkmal des Teilnehmers zum Zwecke der Authentifizierung bzw. Autorisierung vereinbart werden.

2.1 Personalisierte Sicherheitsmerkmale

Personalisierte Sicherheitsmerkmale sind personalisierte Merkmale, die die Bank dem Teilnehmer zum Zwecke der Authentifizierung bzw. Autorisierung bereitstellt. Dies sind beispielsweise:

- die persönliche Identifikationsnummer (PIN) oder der Nutzungscode für die elektronische Signatur und
- einmal verwendbare Transaktionsnummern (TAN).

2.2 Zahlungsinstrumente

Zahlungsinstrumente sind personalisierte Instrumente oder Verfahren, deren Verwendung zwischen der Bank und dem Kontoinhaber vereinbart wurden und die vom Teilnehmer zur Erteilung eines OnlineBanking-Auftrags verwendet werden. Insbesondere mittels folgender Zahlungsinstrumente kann die TAN bzw. die elektronische Signatur dem Teilnehmer zur Verfügung gestellt werden:

- TAN-Generator, der Bestandteil einer Chipkarte oder eines anderen elektronischen Geräts zur Erzeugung von TAN ist,
- OnlineBanking-App auf einem mobilen Endgerät (z. B. Mobiltelefon) zum Empfang oder zur Erzeugung von TAN,
- mobiles Endgerät (z. B. Mobiltelefon) zum Empfang von TAN per SMS (mobileTAN),
- Chipkarte mit Signaturfunktion oder
- sonstiges Zahlungsinstrument, auf dem sich Signaturschlüssel befinden.

3. Zugang zum OnlineBanking

Der Teilnehmer erhält Zugang zum OnlineBanking, wenn

- der Teilnehmer die Kontonummer oder seine individuelle Teilnehmerkennung (PSD-Key oder Alias) und seine PIN oder elektronische Signatur übermittelt oder sein biometrisches Merkmal eingesetzt hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (siehe Nummer 9) vorliegt.

Nach Gewährung des Zugangs zum OnlineBanking kann der Teilnehmer Informationen abrufen oder Aufträge erteilen. Die Sätze 1 und 2 gelten auch, wenn Zahlungsaufträge über einen Zahlungsauslösedienst ausgelöst und Zahlungskontoinformationen über einen Kontoinformationsdienst angefordert werden (siehe Nummer 1 Absatz 1 Satz 3).

4. OnlineBanking-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss OnlineBanking-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit dem von der Bank bereitgestellten Personalisierten Sicherheitsmerkmal (z. B. TAN oder elektronische Signatur) oder mit dem vereinbarten biometrischen Sicherheitsmerkmal autorisieren und der Bank mittels OnlineBanking übermitteln, sofern mit der Bank nichts anderes vereinbart wurde. Die Bank bestätigt mittels OnlineBanking den Eingang des Auftrags. Die Sätze 1 und 2 gelten auch, wenn der Inhaber eines Zahlungskontos und dessen Bevollmächtigte Zahlungsaufträge über einen Zahlungsauslösedienst (siehe Nummer 1 Absatz 1 Satz 3) auslösen und übermitteln.

4.2 Widerruf von Aufträgen

Die Widerrufbarkeit eines OnlineBanking-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr). Der Widerruf von Aufträgen kann nur außerhalb des OnlineBanking erfolgen, es sei denn, die Bank sieht eine Widerrufmöglichkeit im OnlineBanking ausdrücklich vor.

5. Bearbeitung von OnlineBanking-Aufträgen durch die Bank

(1) Die Bearbeitung der OnlineBanking-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) auf der OnlineBanking-Seite der Bank oder im „Preis- und Leistungsverzeichnis" bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem auf der OnlineBanking-Seite der Bank angegebenen oder im „Preis- und Leistungsverzeichnis" bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis" der Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Die Bank wird den Auftrag ausführen, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat den Auftrag autorisiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das OnlineBanking-Datenformat ist eingehalten.
- Das gesondert vereinbarte OnlineBanking-Verfügungslimit ist nicht überschritten.
- Die weiteren Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Sonderbedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Satz 1 vor, führt die Bank die OnlineBanking-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Bedingungen für den Überweisungsverkehr, Bedingungen für das Wertpapiergeschäft) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den OnlineBanking-Auftrag nicht ausführen und dem Teilnehmer eine Information über die Nichtausführung und - soweit möglich - über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, mittels OnlineBanking zur Verfügung stellen.

6. Information des Kontoinhabers über OnlineBanking-Verfügungen

Die Bank unterrichtet den Kontoinhaber mindestens einmal monatlich über die mittels OnlineBanking getätigten Verfügungen auf dem für Kontoinformationen vereinbarten Weg.

7. Sorgfaltspflichten des Teilnehmers

7.1 Technische Verbindung zum OnlineBanking

Der Teilnehmer ist verpflichtet, die technische Verbindung zum OnlineBanking über die von der Bank gesondert mitgeteilten OnlineBanking-Zugangskanäle (z. B. Internetadresse) herzustellen. Der Inhaber eines Zahlungskontos und dessen Bevollmächtigte können zur Auslösung von Zahlungsaufträgen und zur Anforderung von Zahlungskontoinformationen auch über einen von ihnen ausgewählten Zahlungsauslösedienst oder Kontoinformationsdienst (siehe Nummer 1 Absatz 1 Satz 3) die technische Verbindung zum OnlineBanking herstellen.

7.2 Geheimhaltung der Personalisierten Sicherheitsmerkmale und sichere Aufbewahrung der Zahlungsinstrumente

(1) Der Teilnehmer hat

- seine Personalisierten Sicherheitsmerkmale (siehe Nummer 2.1) geheim zu halten sowie
- sein Zahlungsinstrument (siehe Nummer 2.2) vor dem Zugriff anderer Personen sicher zu verwahren.

Denn jede andere Person, die im Besitz des Zahlungsinstruments ist, kann in Verbindung mit der Kenntnis des dazugehörigen Personalisierten Sicherheitsmerkmals das OnlineBanking-Verfahren missbräuchlich nutzen.

Die Geheimhaltungspflicht bezüglich des Personalisierten Sicherheitsmerkmals nach Satz 1 gilt nicht für den Inhaber eines Zahlungskontos und dessen Bevollmächtigte gegenüber Zahlungsauslösediensten und Kontoinformationsdiensten (siehe Nummer 1 Absatz 1 Satz 3), wenn diese Zahlungsaufträge über einen Zahlungsauslösedienst auslösen oder Zahlungskontoinformationen über einen Kontoinformationsdienst anfordern.

(2) Insbesondere ist Folgendes zum Schutz des Personalisierten Sicherheitsmerkmals sowie des Zahlungsinstruments zu beachten:

- Die Personalisierten Sicherheitsmerkmale dürfen nicht ungesichert elektronisch gespeichert werden.
- Bei Eingabe der Personalisierten Sicherheitsmerkmale ist sicherzustellen, dass andere Personen diese nicht ausspähen können.
- Die Personalisierten Sicherheitsmerkmale dürfen nicht per E-Mail oder anderen Telekommunikationsmitteln weitergegeben werden.
- Das Personalisierte Sicherheitsmerkmal (z. B. PIN) darf nicht zusammen mit dem Zahlungsinstrument verwahrt werden.
- Der Teilnehmer darf zur Autorisierung z. B. eines Auftrags oder der Aufhebung einer Sperre nicht mehr als eine TAN verwenden.
- Beim mobileTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das OnlineBanking genutzt werden.

7.3 Sicherheitshinweise der Bank

Der Teilnehmer muss die Sicherheitshinweise der Bank zum OnlineBanking, insbesondere die Maßnahmen zum Schutz der eingesetzten Hard- und Software (Kundensystem), beachten.

7.4 Kontrolle der Auftragsdaten mit von der Bank angezeigten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem OnlineBanking-Auftrag (z. B. Betrag, Kontonummer des Zahlungsempfängers, Wertpapierkennnummer) im Kundensystem oder über ein anderes Gerät des Teilnehmers (z. B. Mobiltelefon, Chipkartenlesegerät mit Display) zur Bestätigung anzeigt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der angezeigten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen. Bei Feststellung von Abweichungen ist die Transaktion abzubrechen.

8. Anzeige- und Unterrichtungspflichten

8.1 Sperranzeige

(1) Stellt der Teilnehmer den Verlust oder den Diebstahl des Zahlungsinstruments, die missbräuchliche Verwendung oder die sonstige nicht autorisierte Nutzung seines Zahlungsinstruments oder eines seiner Personalisierten Sicherheitsmerkmale fest, muss der Teilnehmer die Bank hierüber unverzüglich unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.

(3) Hat der Teilnehmer den Verdacht, dass eine andere Person unberechtigt

- den Besitz an seinem Zahlungsinstrument oder die Kenntnis seines Personalisierten Sicherheitsmerkmals erlangt hat oder
- das Zahlungsinstrument oder das Personalisierte Sicherheitsmerkmal verwendet,

muss er ebenfalls eine Sperranzeige abgeben.

8.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Kontoinhaber hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

9. Nutzungssperre

9.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 8.1,

- den OnlineBanking-Zugang für ihn oder alle Teilnehmer oder
- sein Zahlungsinstrument.

9.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den OnlineBanking-Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den OnlineBanking-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit des Zahlungsinstruments oder des Personalisierten Sicherheitsmerkmals dies rechtfertigen oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung des Zahlungsinstruments besteht.

(2) Die Bank wird den Konto-/Depotinhaber unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

9.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder das Personalisierte Sicherheitsmerkmal bzw. das Zahlungsinstrument austauschen, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Konto-/Depotinhaber unverzüglich.

9.4 Automatische Sperre eines Chip-basierten Zahlungsinstruments

(1) Die Chipkarte mit Signaturfunktion sperrt sich selbst, wenn der Nutzungscode für die elektronische Signatur dreimal in Folge falsch eingegeben wird.

(2) Ein TAN-Generator als Bestandteil einer Chipkarte, der die Eingabe eines eigenen Nutzungscodes erfordert, sperrt sich selbst, wenn dieser dreimal in Folge falsch eingegeben wird.

(3) Die in den Absätzen 1 und 2 genannten Zahlungsinstrumente können dann nicht mehr für das OnlineBanking genutzt werden. Der Teilnehmer kann sich mit der Bank in Verbindung setzen, um die Nutzungsmöglichkeiten des OnlineBanking wiederherzustellen.

10. Haftung

10.1 Haftung der Bank bei einer nicht autorisierten OnlineBanking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten OnlineBanking-Verfügung

Die Haftung der Bank bei einer nicht autorisierten OnlineBanking-Verfügung und einer nicht, fehlerhaft oder verspätet ausgeführten OnlineBanking-Verfügung richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für das Wertpapiergeschäft).

10.2 Haftung des Konto-/Depotinhabers bei missbräuchlicher Nutzung eines Personalisierten Sicherheitsmerkmals oder eines Zahlungsinstruments

10.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruhen nicht autorisierte Zahlungsvorgänge vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen oder sonst abhanden gekommenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Verwendung eines Zahlungsinstruments, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 50 Euro, ohne dass es darauf ankommt, ob den Teilnehmer ein Verschulden trifft.

(2) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach Absatz 1 verpflichtet, wenn

- es ihm nicht möglich gewesen ist, den Verlust, den Diebstahl, das Abhandenkommen oder eine sonstige missbräuchliche Verwendung des Zahlungsinstruments vor dem nicht autorisierten Zahlungsvorgang zu bemerken, oder
- der Verlust des Zahlungsinstruments durch einen Angestellten, einen Agenten, eine Zweigniederlassung eines Zahlungsdienstleisters oder eine sonstige Stelle, an die Tätigkeiten des Zahlungsdienstleisters ausgelagert wurden, verursacht worden ist.

(3) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer in betrügerischer Absicht gehandelt oder seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen vorsätzlich oder grob fahrlässig verletzt, trägt der Kontoinhaber abweichend von den Absätzen 1 und 2 den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere vorliegen, wenn er

- den Verlust oder Diebstahl des Zahlungsinstruments oder die missbräuchliche Nutzung des Zahlungsinstruments oder des Personalisierten Sicherheitsmerkmals der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (siehe Nummer 8.1 Absatz 1),
- das Personalisierte Sicherheitsmerkmal ungesichert elektronisch gespeichert hat (siehe Nummer 7.2 Absatz 2, 1. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal nicht geheim gehalten hat und der Missbrauch dadurch verursacht wurde (siehe Nummer 7.2 Absatz 1),

- das Personalisierte Sicherheitsmerkmal per E-Mail oder anderen Telekommunikationsmitteln weitergegeben hat (siehe Nummer 7.2 Absatz 2, 3. Spiegelstrich),
- das Personalisierte Sicherheitsmerkmal auf dem Zahlungsinstrument vermerkt oder zusammen mit diesem verwahrt hat (siehe Nummer 7.2 Absatz 2, 4. Spiegelstrich),
- mehr als eine TAN zur Autorisierung eines Auftrags verwendet (siehe Nummer 7.2 Absatz 2, 5. Spiegelstrich),
- beim mobileTAN-Verfahren das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), auch für das OnlineBanking nutzt (siehe Nummer 7.2 Absatz 2, 6. Spiegelstrich).

(4) Abweichend von den Absätzen 1 und 3 ist der Kontoinhaber nicht zum Schadenersatz verpflichtet, wenn die Bank vom Teilnehmer eine starke Kundenauthentifizierung nach § 1 Absatz 24 Zahlungsdiensteaufsichtsgesetz nicht verlangt hat, obwohl die Bank zur starken Kundenauthentifizierung nach § 68 Absatz 4 Zahlungsdiensteaufsichtsgesetz verpflichtet war. Eine starke Kundenauthentifizierung erfordert insbesondere die Verwendung von zwei voneinander unabhängigen Elementen aus den Kategorien Wissen (etwas, das der Teilnehmer weiß, z. B. PIN), Besitz (etwas, das der Teilnehmer besitzt, z. B. TAN-Generator) oder Inhärenz (etwas, das der Teilnehmer ist, z. B. Fingerabdruck).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den mitgeteilten Verfügungsrahmen.

(6) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 8.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte.

(7) Die Absätze 2 und 4 bis 6 finden keine Anwendung, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

(8) Ist der Kontoinhaber kein Verbraucher, gilt ergänzend Folgendes:
- Der Kontoinhaber haftet für Schäden aufgrund von nicht autorisierten Zahlungsvorgängen über die Haftungsgrenze von 50 Euro nach Absatz 1 und 3 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Bedingungen verstoßen hat.
- Die Haftungsbeschränkung in Absatz 2 erster Spiegelstrich findet keine Anwendung.

10.2.2 Haftung des Depotinhabers bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige
Beruhen nicht autorisierte Wertpapiertransaktionen vor der Sperranzeige auf der Nutzung eines verlorengegangenen oder gestohlenen Zahlungsinstruments oder auf der sonstigen missbräuchlichen Nutzung des Personalisierten Sicherheitsmerkmals oder des Zahlungsinstruments und ist der Bank hierdurch ein Schaden entstanden, haften der Depotinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

10.2.3 Haftung der Bank ab der Sperranzeige
Sobald die Bank eine Sperranzeige des Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte OnlineBanking-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

10.2.4 Haftungsausschluss
Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können.

11. Außergerichtliche Streitschlichtung und sonstige Beschwerdemöglichkeit
Für die Beilegung von Streitigkeiten mit der Bank kann sich der Teilnehmer an die im „Preis- und Leistungsverzeichnis“ näher bezeichneten Streitschlichtungs- oder Beschwerdestellen wenden.

Sonderbedingungen für die Nutzung des elektronischen Postfachs

PSD Bank München eG, Sitz Augsburg

Stand: Juli 2017

1. Das elektronische Postfach
Die Bank bietet dem Kunden die Möglichkeit eines Zugangs zu seinen bei der Bank geführten Konten und Depots über das Internet. Im Rahmen der Geschäftsbeziehung zwischen der Bank und dem Kunden, der für die Nutzung des elektronischen Postfachs freigeschaltet ist, gilt das elektronische Postfach als Kommunikationsweg. Der Kunde kann das elektronische Postfach im bereitgestellten Funktionsumfang nutzen. Wenn der Bevollmächtigte Zugang zum Online Banking hat, ist ihm die Nutzung des elektronischen Postfachs in gleicher Weise wie dem Kontoinhaber bzw. den Kontoinhabern gestattet.

2. Übermittlung von Konto- und Kundendokumenten
Bei Nutzung des elektronischen Postfachs werden dem Kunden sämtliche Konto- und Kundendokumente dort eingestellt. Dies umfasst beispielsweise Konto- und Depotauszüge, Rechnungsabschlüsse, Kreditkartenabrechnungen sowie Angebote zur Änderung der Allgemeine Geschäftsbedingungen, Sonderbedingungen oder Entgelte.

3. Verzicht auf papierhafte Konto- und Kundendokumente
Die Bank kann ihre Informationsverpflichtungen aus der Geschäftsbeziehung dadurch erfüllen, dass sie Informationen elektronisch in den Posteingang übersendet. Die Übersendung der Mitteilung erfolgt insbesondere durch Einstellung von Dateien im PDF-Format in das elektronische Postfach. Die Bank wird die Informationen, die sie im Posteingang bereitstellt, grundsätzlich nicht zusätzlich papierhaft versenden. Der Kunde verzichtet ausdrücklich auf den postalischen Versand dieser Informationen, wenn die entsprechenden Konten auf das elektronische Postfach umgestellt sind. Die Bank bleibt dazu berechtigt, dem Kunden Dokumente per Post zuzusenden, wenn sie dies unter Berücksichtigung der Kundeninteressen für zweckmäßig hält oder es aus rechtlichen Gründen erforderlich ist.

4. Mitwirkungspflichten des Kunden
Der Kunde ist verpflichtet, regelmäßig und zeitnah die Informationen im Posteingang abzurufen und die Inhalte zu prüfen. Er hat der Bank eventuelle Unstimmigkeiten unverzüglich anzuzeigen.

5. Kündigung
Der Kunde kann die Nutzung des elektronischen Postfachs jederzeit in Textform ohne Einhaltung einer Frist kündigen. Die Bank kann die Nutzung des elektronischen Postfachs jederzeit mit einer Frist von 2 Monaten kündigen, es sei denn, es liegt ein wichtiger Grund vor, der sie zu einer außerordentlichen Kündigung berechtigen würde. Ein wichtiger Grund liegt insbesondere dann vor, wenn es der Bank auch unter angemessener Berücksichtigung der Belange des Kunden unzumutbar erscheint, den elektronischen Postfach-Dienst fortzusetzen.
Die Bank wird nach dem Wirksamwerden einer Kündigung alle Informationen im Rahmen der Geschäftsbeziehung per Post an die vom Kunden angegebene Anschrift versenden. Im Falle einer fristlosen Kündigung durch den Kunden kann dieses jedoch erst nach einer angemessenen Bearbeitungszeit erfolgen. Die Bank ist nicht verpflichtet, dem Kunden die im Zeitpunkt des Wirksamwerdens der Kündigung im Posteingang befindlichen Informationen nachträglich postalisch zuzusenden. Die Entgelte ergeben sich aus dem „Preis- und Leistungsverzeichnis“.

6. Anerkennung durch Finanzbehörden
Kunden, die handels- und steuerrechtlichen Aufbewahrungspflichten unterliegen, sollten sich bei einem Angehörigen der steuerberatenden Berufe informieren, was im Fall des Bezugs von elektronischen Dokumenten (z. B. Kontoauszügen) zur Erfüllung dieser Pflichten zu beachten ist.
Die Informationen können nach ihrer Übermittlung in den Posteingang nicht verändert werden. Die Bank garantiert die Unveränderbarkeit der in das elektronische Postfach bereit gestellten Daten. Diese Garantie gilt jedoch nicht, sofern die Daten außerhalb des elektronischen Postfachs gespeichert oder aufbewahrt werden. Dabei ist zu beachten, dass ein Ausdruck eines Dokuments aufgrund der individuellen Hard- oder Softwareeinstellung von der Darstellung am Bildschirm abweichen kann. Soweit die Dokumente verändert werden oder in veränderter Form in Umlauf gebracht werden, haftet die Bank hierfür nicht.

Sonderbedingungen für PSD ServiceDirekt (TelefonBanking)

PSD Bank München eG, Sitz Augsburg

Stand: Februar 2017

1. Leistungsangebot

(1) Konto-/Depotinhaber und Bevollmächtigte werden im Folgenden einheitlich als „Teilnehmer“ bezeichnet. Konto und Depot werden im Folgenden einheitlich als „Konto“ bezeichnet.

(2) Der Teilnehmer kann Bankgeschäfte im Rahmen von PSD ServiceDirekt mittels Telefon in dem von der Bank angebotenen Umfang abwickeln. Zudem kann er Informationen der Bank mittels PSD ServiceDirekt abrufen.
Die im PSD ServiceDirekt erteilten Wertpapieraufträge werden ohne Beratung durchgeführt.
Die Berechtigung zur Erteilung von Wertpapieraufträgen mittels PSD ServiceDirekt bedarf einer separaten Rahmenvereinbarung.

(3) Zur Nutzung von PSD ServiceDirekt gelten die mit der Bank gesondert vereinbarten Verfügungslimite. Eine Änderung dieser Limite kann der Teilnehmer mit seiner Bank gesondert vereinbaren.

2. Voraussetzungen zur Nutzung von PSD ServiceDirekt

Der Teilnehmer benötigt für die Abwicklung von Bankgeschäften mittels PSD ServiceDirekt die mit der Bank vereinbarte persönliche Identifikationsnummer (PIN), um sich gegenüber der Bank als berechtigter Teilnehmer auszuweisen und Aufträge zu autorisieren (vgl. Nummer 4.1).

3. Zugang zum PSD ServiceDirekt

Der Teilnehmer erhält Zugang zum PSD ServiceDirekt mittels Telefon, wenn

- der Teilnehmer die Kunden-/Kontonummer oder seine individuelle Kundenkennung (PSD Key oder Alias) nennt und seine PIN über die Tastatur des Telefons eingegeben hat,
- die Prüfung dieser Daten bei der Bank eine Zugangsberechtigung des Teilnehmers ergeben hat und
- keine Sperre des Zugangs (vgl. Nummer 7) vorliegt.

Nach Gewährung des Zugangs zum PSD ServiceDirekt kann der Teilnehmer Informationen abrufen oder Aufträge erteilen.
Die Bank darf sich zur Durchführung von PSD ServiceDirekt-Geschäften eines Erfüllungsgehilfen bedienen, der die technische Abwicklung für die Bank durch eine zentrale Auftragsannahme vornimmt. Dieser Erfüllungsgehilfe ist berechtigt, im Rahmen der Abwicklung der Aufträge Einsicht in Kundenkonten zu nehmen.

4. PSD ServiceDirekt-Aufträge

4.1 Auftragserteilung und Autorisierung

Der Teilnehmer muss PSD ServiceDirekt-Aufträge (z. B. Überweisungen) zu deren Wirksamkeit mit der vereinbarten PIN autorisieren und der Bank mittels Telefon übermitteln. Der Auftrag wird am Telefon bestätigt.

4.2 Widerruf von PSD ServiceDirekt-Aufträgen

Die Widerrufbarkeit eines PSD ServiceDirekt-Auftrags richtet sich nach den für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr).

5. Bearbeitung von PSD ServiceDirekt-Aufträgen durch die Bank

(1) Die Bearbeitung der PSD ServiceDirekt-Aufträge erfolgt an den für die Abwicklung der jeweiligen Auftragsart (z. B. Überweisung) im „Preis- und Leistungsverzeichnis“ bekannt gegebenen Geschäftstagen im Rahmen des ordnungsgemäßen Arbeitslaufes. Geht der Auftrag nach dem im „Preis- und Leistungsverzeichnis“ bestimmten Zeitpunkt (Annahmefrist) ein oder fällt der Zeitpunkt des Eingangs nicht auf einen Geschäftstag gemäß „Preis- und Leistungsverzeichnis“ der Bank, so gilt der Auftrag als am darauffolgenden Geschäftstag zugegangen. Die Bearbeitung beginnt erst an diesem Tag.

(2) Der Auftrag wird ausgeführt, wenn folgende Ausführungsbedingungen vorliegen:

- Der Teilnehmer hat sich mit seiner PIN legitimiert.
- Die Berechtigung des Teilnehmers für die jeweilige Auftragsart (z. B. Wertpapierorder) liegt vor.
- Das gesondert vereinbarte PSD ServiceDirekt-Verfügungslimit ist nicht überschritten.
- Die Ausführungsvoraussetzungen nach den für die jeweilige Auftragsart maßgeblichen Sonderbedingungen (z. B. ausreichende Kontodeckung gemäß den Sonderbedingungen für den Überweisungsverkehr) liegen vor.

Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 vor, führt die Bank die PSD ServiceDirekt-Aufträge nach Maßgabe der Bestimmungen der für die jeweilige Auftragsart geltenden Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für Wertpapiergeschäfte) aus.

(3) Liegen die Ausführungsbedingungen nach Absatz 2 Satz 1 nicht vor, wird die Bank den PSD ServiceDirekt-Auftrag nicht ausführen und dem Teilnehmer über die Nichtausführung und – soweit möglich – über deren Gründe und die Möglichkeiten, mit denen Fehler, die zur Ablehnung geführt haben, berichtigt werden können, eine Information zur Verfügung stellen.

6. Sorgfaltspflichten des Teilnehmers

6.1 Technische Verbindung zum PSD ServiceDirekt

Der Teilnehmer ist verpflichtet, die Verbindung zum PSD ServiceDirekt nur über die von der Bank gesondert mitgeteilten TelefonBanking-Telefonnummern herzustellen.

6.2 Geheimhaltung des Personalisierten Sicherheitsmerkmals

(1) Der Teilnehmer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN erlangt. Denn jede andere Person, die im Besitz der PIN ist, hat die Möglichkeit, den PSD ServiceDirekt missbräuchlich zu nutzen.

(2) Insbesondere ist Folgendes zum Schutz der PIN zu beachten:

- Die Weitergabe der PIN an andere Personen ist nicht zulässig.
- Die im Telefonspeicher gespeicherte PIN ist zu löschen oder zu überschreiben, damit nachfolgende Nutzer des Geräts nicht diese ausspähen können.
- Die PIN darf nicht elektronisch gespeichert werden (z. B. im Kundensystem).
- Bei Eingabe bzw. Übermittlung der PIN ist sicherzustellen, dass andere Personen diese nicht ausspähen bzw. mithören können.
- Die PIN darf nicht außerhalb des PSD ServiceDirekt-Verfahrens weitergegeben werden, also beispielsweise nicht per E-Mail.

6.3 Änderung der PIN

Der Teilnehmer ist verpflichtet, bei erstmaliger Nutzung seine PIN zu ändern. Darüber hinaus ist der Teilnehmer jederzeit berechtigt, seine PIN zu ändern.

6.4 Kontrolle der Auftragsdaten mit von der Bank mitgeteilten Daten

Soweit die Bank dem Teilnehmer Daten aus seinem PSD ServiceDirekt-Auftrag (z. B. Betrag, IBAN des Zahlungsempfängers, Wertpapierkennnummer) telefonisch wiederholt, ist der Teilnehmer verpflichtet, vor der Bestätigung die Übereinstimmung der mitgeteilten Daten mit den für die Transaktion vorgesehenen Daten zu prüfen.

7. Anzeige- und Unterrichtungspflichten

7.1 Sperranzeige

(1) Stellt der Teilnehmer

- den Verlust oder Diebstahl der PIN,
- die missbräuchliche Verwendung oder
- die sonstige nicht autorisierte Nutzung seiner PIN

fest oder hat er den Verdacht, dass eine andere Person von seiner PIN Kenntnis erhalten hat, ist der Teilnehmer verpflichtet, die Bank hierüber unverzüglich zu unterrichten (Sperranzeige). Der Teilnehmer kann der Bank eine Sperranzeige jederzeit auch über die gesondert mitgeteilten Kontaktdaten abgeben.

(2) Der Teilnehmer hat jeden Diebstahl oder Missbrauch unverzüglich bei der Polizei zur Anzeige zu bringen.

7.2 Unterrichtung über nicht autorisierte oder fehlerhaft ausgeführte Aufträge

Der Teilnehmer hat die Bank unverzüglich nach Feststellung eines nicht autorisierten oder fehlerhaft ausgeführten Auftrags hierüber zu unterrichten.

8. Nutzungssperre

8.1 Sperre auf Veranlassung des Teilnehmers

Die Bank sperrt auf Veranlassung des Teilnehmers, insbesondere im Fall der Sperranzeige nach Nummer 7.1, den PSD ServiceDirekt-Zugang für ihn oder alle Teilnehmer.

8.2 Sperre auf Veranlassung der Bank

(1) Die Bank darf den Zugang für einen Teilnehmer sperren, wenn

- sie berechtigt ist, den PSD ServiceDirekt-Vertrag aus wichtigem Grund zu kündigen,
- sachliche Gründe im Zusammenhang mit der Sicherheit der PIN dies rechtfertigen,
  oder
- der Verdacht einer nicht autorisierten oder einer betrügerischen Verwendung der PIN besteht.

(2) Die Bank wird den Teilnehmer unter Angabe der hierfür maßgeblichen Gründe möglichst vor, spätestens jedoch unverzüglich nach der Sperre unterrichten.

8.3 Aufhebung der Sperre

Die Bank wird eine Sperre aufheben oder dem Teilnehmer eine neue PIN zusenden, wenn die Gründe für die Sperre nicht mehr gegeben sind. Hierüber unterrichtet sie den Teilnehmer unverzüglich.

8.4 Automatische Sperre der PIN

Das System sperrt die PIN automatisch, wenn der Teilnehmer dreimal hintereinander eine falsche PIN eingibt. Auf Anforderung erhält der Teilnehmer eine neue PIN zugesandt.

9. Haftung

9.1 Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten PSD ServiceDirekt-Verfügungen

Die Haftung der Bank bei nicht autorisierten und nicht oder fehlerhaft ausgeführten PSD ServiceDirekt-Verfügungen richtet sich nach den für die jeweilige Auftragsart vereinbarten Sonderbedingungen (z. B. Sonderbedingungen für den Überweisungsverkehr, Sonderbedingungen für Wertpapiergeschäfte).

9.2 Haftung des Kontoinhabers bei missbräuchlicher Nutzung seiner PIN

9.2.1 Haftung des Kontoinhabers für nicht autorisierte Zahlungsvorgänge vor der Sperranzeige

(1) Beruht ein nicht autorisierter Zahlungsvorgang vor der Sperranzeige auf einer verlorengegangenen, gestohlenen oder sonst abhanden gekommenen PIN, haftet der Kontoinhaber für den der Bank hierdurch entstehenden Schaden bis zu einem Betrag von 150 Euro, wenn der Teilnehmer seine Pflicht zur sicheren Aufbewahrung der PIN schuldhaft verletzt hat.

(2) Ist der Kontoinhaber kein Verbraucher, haftet er für Schäden aufgrund von nicht autorisierten Zahlungen über die Haftungsgrenze von 150 Euro nach Absatz 1 hinaus, wenn der Teilnehmer fahrlässig oder vorsätzlich gegen seine Anzeige- und Sorgfaltspflichten nach diesen Sonderbedingungen gehandelt hat.

(3) Der Kontoinhaber ist nicht zum Ersatz des Schadens nach den Absätzen 1, 2 und 3 verpflichtet, wenn der Teilnehmer die Sperranzeige nach Nummer 7.1 nicht abgeben konnte, weil die Bank nicht die Möglichkeit zur Entgegennahme der Sperranzeige sichergestellt hatte und der Schaden dadurch eingetreten ist.

(4) Kommt es vor der Sperranzeige zu nicht autorisierten Zahlungsvorgängen und hat der Teilnehmer seine Sorgfaltspflichten nach diesen Sonderbedingungen vorsätzlich oder grob fahrlässig verletzt oder in betrügerischer Absicht gehandelt, trägt der Kontoinhaber den hierdurch entstandenen Schaden in vollem Umfang. Grobe Fahrlässigkeit des Teilnehmers kann insbesondere dann vorliegen, wenn er

- den Verlust oder Diebstahl der PIN oder die missbräuchliche Nutzung der PIN der Bank nicht unverzüglich anzeigt, nachdem er hiervon Kenntnis erlangt hat (vgl. Nummer 7.1 Absatz 1),
- den Telefonspeicher nicht gelöscht oder überschrieben hat und daher eine andere Person Kenntnis von der PIN erlangen könnte (vgl. Nummer 6.2 Absatz 2 1. Spiegelstrich),
- die PIN einer anderen Person mitgeteilt und der Missbrauch dadurch verursacht wurde (vgl. Nummer 7.2 Absatz 1 Satz 1),
- die PIN außerhalb des ServiceDirekt-Verfahrens, beispielsweise per E-Mail, weitergegeben hat (vgl. Nummer 6.2 Absatz 2, 3. Spiegelstrich).

(5) Die Haftung für Schäden, die innerhalb des Zeitraums, für den der Verfügungsrahmen gilt, verursacht werden, beschränkt sich jeweils auf den vereinbarten Verfügungsrahmen.

9.2.2 Haftung bei nicht autorisierten Wertpapiertransaktionen vor der Sperranzeige

Beruht eine nicht autorisierte Wertpapiertransaktion vor der Sperranzeige auf der Nutzung einer verlorengegangenen, gestohlenen oder sonst abhanden gekommenen PIN oder sonstigen missbräuchlichen Nutzung der PIN und ist der Bank hierdurch ein Schaden entstanden, haften der Kontoinhaber und die Bank nach den gesetzlichen Grundsätzen des Mitverschuldens.

9.2.3 Haftung der Bank ab der Sperranzeige

Sobald die Bank eine Sperranzeige des Teilnehmers erhalten hat, übernimmt sie alle danach durch nicht autorisierte PSD ServiceDirekt-Verfügungen entstehenden Schäden. Dies gilt nicht, wenn der Teilnehmer in betrügerischer Absicht gehandelt hat.

9.2.4 Haftungsausschluss

Haftungsansprüche sind ausgeschlossen, wenn die einen Anspruch begründenden Umstände auf einem ungewöhnlichen und unvorhersehbaren Ereignis beruhen, auf das diejenige Partei, die sich auf dieses Ereignis beruft, keinen Einfluss hat, und dessen Folgen trotz Anwendung der gebotenen Sorgfalt von ihr nicht hätten vermieden werden können. Die Bank übernimmt keine Haftung dafür, dass eine Teilnahme am PSD ServiceDirekt vorübergehend oder auf Dauer nicht möglich ist, sofern die Störung nicht auf Vorsatz oder grober Fahrlässigkeit beruht.

10. Telefonaufzeichnung

Der Teilnehmer ist damit einverstanden, dass die Bank die im Rahmen des PSD ServiceDirekt geführten Telefonate sowie die von ihm über die Tastatur des Telefons eingegebenen Ziffern (ausgenommen PIN) aufzeichnet und aufbewahrt. Dies ist zur ordnungsgemäßen Auftragsbearbeitung und aus Beweisgründen erforderlich.

11. Vertragsdauer / Kündigung

Der Vertrag wird auf unbestimmte Zeit geschlossen. Eine Kündigung oder Einschränkung des Vertrages kann von Seiten der Bank unter Einhaltung einer Kündigungsfrist von vier Wochen erklärt werden. Eine Kündigung des Vertrages kann seitens des Teilnehmers jederzeit unter Einhaltung einer vierwöchigen Kündigungsfrist in Textform erklärt werden. Das Recht zur Kündigung aus wichtigem Grund bleibt davon unberührt.